6

Enacting Internet Governance: Power and Communities over Time

The previous chapters showed that the nascent order around Internet governance (IG)—mired in political stakes and built in distinctive phases—matured and crystallized as part of a global dialogue. The diversification of approaches to governance characterized the World Summit on Information Society (WSIS) decade phase of Internet development. Soft instruments, especially discursive and operative modelling tools, were deployed to influence the behaviour of others in this space, mobilized primarily around cybersecurity and civil liberties. Multiple sets of rules and norms discussed across partnerships, from the national to the global scale, entangled to shape the Internet as we know it today. The key transformation compared to previous decades was the understanding that the Internet was ultimately a social and political field of action.

In recent years, the underlying business structure of the Internet came on the radar of regulators more prominently. The oligopolistic position of dominant Internet companies has led to a so-called 'tech backlash' in public discourse: a more careful scrutiny of their activities and the imposition of financial sanctions. The potential for digital market dominance, be it by Western or by Chinese companies, had long been foreseen. In the words of Freedman (2012, 115), 'one thing that has remained constant on the Internet is the structure of a "winner takes all" market which systematizes the need for huge concentrations of online and offline capital'. The policy responses have ranged from imposing stricter taxation rules and defining employment rights in the platform economy to sanctioning anti-competitive behaviour and data protection breaches. Self-regulatory approaches continue to appeal in newer areas of fast technological development such as cloud computing, but all-encompassing regulation on issues such as data protection brings about a horizontal baseline.

Currently, the trust in the effectiveness and power of multi-stakeholder partnerships has diminished. The vision of a public Internet as a force for good

and empowerment has grown to be more nuanced. 'From the Arab Spring to the Occupy movements, from Pegida and the jihadists to the European Indignados, the contemporary Internet is a space for commodification, a vehicle of propaganda, and a tool for political liberation, all at the same time', concluded Smyrnaios (2018, 6). Likewise, the credo of participatory politics via social platforms like Twitter and Facebook (Morozov 2013) was strongly challenged by the advent of algorithmic manipulation, considered a threat to democratic systems. The disclosures of electoral influencing in the campaigns leading up to the Brexit referendum and the US presidential elections in 2016 via algorithms raised concerns that 'filter bubbles' and mandated choices restructure the public sphere, and in particular the deliberation space, in ways previously unaccounted for.

This chapter focuses on locating authority in the field: the first part provides an analysis of the power drivers in a longitudinal perspective, followed by a reflection of the governance dynamics emerging since 2015, with an emphasis on the role of dominant Internet companies and influential states across multiple sub-fields; the strategies of China and India are then comparatively discussed. The second part is dedicated to the formation and perpetuation of the IG community, its characteristics, and decision-making routines. It zooms in on the various meanings of the community referent across different bodies, with the Internet Assigned Numbers Authority (IANA) stewardship transition as a case study, and reviews the three anchoring practices dominating the field.

Power Dynamics and Authority Locus

The diversification of venues for IG discussion that we witnessed starting in 2016 did not put an end to the contest over the re-balancing of power in the field. Once the debate over the management of critical resources ended in September 2016 with the withdrawal of the US government from its IANA stewardship function, the global focus shifted to the unfair distribution of benefits from the digital transformation, in economic, political, and social inclusion terms.

Institutional thickness reached a new height towards the end of 2015, but the phenomenon of multiplication and persistence of international bodies and global regulation did not necessarily result in increased legalization. In the era of cross-sectoral partnerships, soft instruments were preferred to hard law. The adherence to rules entered a new stage, with more frequent references to sanctions rather than norm coherence. As discussed in this section,

rule-based outcomes are continuously sought in IG and the existing global governance structures might not provide satisfactory answers.

From 2015 onwards, power positions solidified. A few Internet companies became more powerful than ever in the field and in the world, topping the industry profits ranking and deciding on the future technical development of the Internet through their investments. Previously, the tensions around the unilateral imposition of rules by one state dominated the IG debates; more recently, emerging powers such as China, Russia, and India strengthened their national approaches and proposed alternative governance principles on the global scale. Other countries and regional blocs also increased their regulatory powers and passed a number of laws with extraterritorial effects, in particular in the areas of cybersecurity, data protection, and privacy. The IG community—made up of representatives of the various sectors—continued to diversify capturing some of these dynamics as they permeated the work of technical bodies and multistakeholder forums.

A Longitudinal Comparison

Looking comparatively at the three periods identified, from the invention of the network to the maturing of a field of action, it becomes apparent that the dominant mode of governance (which sets the tone in a specified time frame) represents only one alternative amid the many governance configurations possible. Arriving at global regulatory coordination via market and state modes, the contemporary IG landscape is unique. Among its most important transformations was the transition from informal to codified procedures and to solidified institutional forms reflecting the growing assortment of international, regional, and national stakeholders. Cybersecurity and civil liberties continue to stand out as two key areas in which cyber norms are still disputed. In the last decade, most efforts have been directed not towards drafting hard law instruments, but towards influencing other actors' behaviour in this space. The effect of modelling has been just as strong through codes of conduct and voluntary schemes stirred by actors operating either individually or in partnership.

Ideologically, two main positions solidified in IG discussions since the 1990s. The first one was built around the exceptionalism of the Internet. It postulated that a global network revolutionizing daily activities across most sectors required a fresh approach, in light of the de-territorialization it fostered. This argument was best expressed by John Perry Barlow in his famous Davos message to the governments of the world:

> You are not welcome among us. You have no sovereignty where we gather. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Cyberspace does not lie within your borders. (Barlow 1996)

On the legal side, that translated into a pursuit of new regulations and 'cyber-laws' at the expense of adapting the existing legislation to tackle relevant online aspects. This approach has been revived several times throughout the 1990s and 2000s, going from a complete rejection of the applicability of 'old' laws (Post 2002) to designing exclusive online guarantees such as the 'right to be forgotten' (Chenou and Radu 2017). The development of an overarching governance system specific to the Internet continues to be an ideal for some of the members of the IG community. While more and more organizations have come to populate the field, there are only a handful core bodies with exclusive attributes for IG. As this study showed so far, the emergence of a highly complex field such as IG rests on a variety of forms of action—from hard law to discursive or operative modelling—implemented by a plethora of new and old institutions.

The second ideological position focused around the need to see the Internet as embedded in real law. This approach was built around understanding how the network has been anchored in geography and how the responsibilities of nation states can be redefined. National, regional, and transnational rules sustained the tremendous success of the Internet since the beginning, in particular as they were covered by the neoliberal mantra prioritizing market development. The new economic models fostered by the Internet were closely linked to the *laissez-faire* regulatory frameworks defined by the Pentagon, at times accepted tacitly, at times vocally contested by other nations. In recent years, the economic and sociopolitical dimensions of the Internet garnered unprecedented attention, challenging the leadership of the United States in the field through the adoption of stronger national regulation targeting data-driven business models.

Making sense of the interconnected code, law, and politics pertinent to IG is an ongoing struggle for anyone participating in these processes. It is thus crucial to understand how critical levers work at various points in time and how they come to define what matters for a community. For instance, in the work of the Internet Engineering Task Force (IETF) and via its Request for Comments (RFCs) practice, standard-making became public—at first out of sheer necessity, subsequently strongly re-enacted for accountability purposes. This set the tone for a series of developments emulating this model, pushing for the open participation of stakeholders across the board, with an implicit understanding of who gets to participate at what stage in the process.

It is thus timely to put into perspective the way in which two dominant actors—companies and states—have evolved in the post-2015 period. Their strategies and expressions of power are indicative of the changes ahead and of the potential for entering a fourth IG evolution phase, built on a new set of principles and introducing novel dynamics.

Private Giants on the Rise

Among the world's most valuable ten firms, seven are Internet giants: five American companies (Apple, Amazon, Alphabet, Microsoft, and Facebook) and two Chinese companies (Tencent and Alibaba). At the time of writing this book, Apple became the world's first public company to be worth $1 trillion (Johnson 2018). These tech companies have long competed for conquering emerging markets and the next generation of Internet users, but after a series of failed connectivity experiments, their attention has shifted towards crossing new frontiers in Internet services and in artificial intelligence (AI). Amazon, Alibaba, and Microsoft are also strengthening their position in cloud computing, a new direction of investments dominating the market.

Many of the top ten companies have introduced projects to bring connectivity to underserved areas of the globe, with mixed results. After a controversial Free Basics proposal that was rejected in India on net neutrality grounds, Facebook deployed the programme in sixty-three countries around the world in partnership with local telecom operators. Despite the explosion of its Space X satellite over sub-Saharan Africa in September 2016, the Facebook experiments continue with its plane-size, solar-powered Internet drone called Aquila. Alphabet's drone program, Project Titan, was terminated in 2017, but work continues for high-altitude balloons in the framework of Project Loon. Microsoft tests unused television airwaves (white space) to reach the unconnected with pilot projects in Jamaica, Namibia, the Philippines, Tanzania, Taiwan, Colombia, the United Kingdom, and the United States.

Technologies like the fifth generation (5G) of mobile networks are of close interest to Chinese companies, which are sending increasingly more representatives to related meetings organized by standardization bodies. They work closely with the government in the framework of China's Belt and Road Initiative, one of the largest ever infrastructure projects covering more than sixty-eight countries. The initiative comprises a 'digital Silk Road' ambitious plan to build anything from fibre-optic cables and mobile networks to smart cities on the multiple water and land corridors thus created. This is achieved with Chinese companies, engineers, and managers, with capacity building provided by Chinese experts.

At the level of Internet architecture, a fundamental change is underway in submarine cable investments. A number of hardware, software, and data-driven companies have participated in consortia to build a large number of the 448 undersea cables in use around the world (at the time of writing). Google, for example, invested in six cables since 2008. This space has been privately owned since the beginning and the telecom operators paying for the deployment of cables set up specific traffic exchange and power sharing arrangements in the 1990s. Since 2016, major investors in cables have been underway by new players: content providers such as Google, Facebook, or Amazon have joined the submarine connectivity race. More and more of these companies are buying important shares in the business or creating their own cables: Google owns 63,605 miles representing 8.5 per cent of the under cables worldwide, and will soon become the first content provider with sole ownership of submarine cables in the industry (BroadbandNow 2018). Facebook and Amazon, together with four more partners, jointly build the Jupiter cable to link the United States to Asia by 2020. These investments are alimenting the cloud computing business, which represents a $60 billion-a-year market, continuously growing with Amazon in the lead (33 per cent share), followed by Microsoft, Google, Alibaba, and IBM (Lohr 2018).

This change at the level of infrastructure has to do with a better quality of service, obtained by moving a copy of the content closer to the user, to avoid transit delays. Yet, according to Huston (2016), this imposes a degree of 'fragmentation in the architecture of the Internet as a result of service delivery specialisation' and restructures the market according to new rules imposed by the big players. Standard-making may also depend entirely on these private content providers turned infrastructure providers in the near future.

Younger Silicon Valley companies, such as Airbnb and Uber, have made their fortune in the sharing economy. The second wave of promising Bay Area companies built their business around the collection and processing of real-time information of demand and supply. In the words of Tom Goodwin (2015):

> Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate.

Ridesharing, apartment or home lending, and re-selling are all peer-to-peer alternatives to owning the good or the service of interest. The difference lies in the use of data to provide added-value and comfort via an online platform. 'Uberisation'—a term derived from the name of an American ridesharing company, Uber—is now applied across the board to designate

the transition to a new economic model based on digital technologies enabling direct exchanges between providers of services and potential customers at lower costs. These business models share three main features: a prevalence of contractual and temporary employment, a digital platform/app for peer-to-peer transactions, and a rating system for evaluating the quality of the service provided.

Examples of companies claiming to take part in the sharing economy abound across many sectors: entertainment (Spotify, Netflix, GameFly), transportation (Uber, Lyft, Zipcar), accommodation (Airbnb, HomeExchange), labour (Mechanical Turk, SkillShare, TaskRabbit), fashion (Fashionhire, Rent the Runaway), etc. According to Parker et al. (2016), the networked business model introduces two innovations: (1) the company no longer creates the end product or service, but focuses on making available a common infrastructure that matches consumers and producers using the knowledge of the market and imposing the rules of governance; (2) the producers of value and consumers of value come from outside the system. The expansion of the 'gig economy' model across different sectors introduced a wave a social experimentation indicative of the extensive power of corporations in the digital world, equalling or exceeding that of governments.

In a span of six years, the prospects of the sharing economy have been critically reassessed. Two dominant narratives have driven the debates on different value propositions: on the one hand, the bright future of automation promised further innovation and entrepreneurship opportunities, as well as flexible schedules and labour market activation, putting technology at work for delivering better products at a lower price. On the other hand, the narrative of medieval exploitation surfaced as an equally strong one: algorithmic ratings, consumer evaluations, and temporary tasks delivered on platforms led to an ever-expanding, precarious on-demand workforce, primarily underemployed (Prassl 2018). The shift from the first to the second narrative has revealed that innovations in the digital economy pose novel and more complex regulatory challenges, not only to the policymakers, but also to the companies themselves.

Uber's enormous exposure to litigation in the majority of jurisdictions in which it operates epitomizes broader dilemmas in assessing the effects of business models on society. Classifying the sharing economy services as information ones (providing the data necessary to link demand and supply) or as part of a regulated industry (transport, hospitality services, etc.) has been the crux of the matter, as it brings forward the applicable regulatory regime: most legal cases are about the employment and labour conditions of those gaining a living this way, as well as e-commerce and trade aspects, including competition, advertising, and licensing. Organizing the digital landscape while fitting

the current societal structure has been an ongoing power struggle, in which the dominant businesses have predominantly argued for exemption from the rules applied to the industries they seek to displace. The gatekeeping function of giant technology companies limits access to alternative models of social and economic organization, although the Internet infrastructure itself does not, in principle, prioritize one over the other.

Alongside infrastructure and digital economy, the third subarea of unprecedented private sector development has been AI. This broad umbrella term refers to the latest and most successful wave of machine learning modelled on neural networks and deep learning. Deployed for purposes as diverse as advancements in medical diagnosis and autonomous driving, this technological breakthrough allowed a number of start-ups—mainly based in the United States, in India, and in China—to build up their profiles. The largest tech companies are either developing their own research unit on AI or acquiring the smaller companies thriving in the field.

In the data-driven economy and in the functioning of AI, algorithms are indispensable. They are deployed across a wide number of services, from technical ones (e.g. spam filtering and advertising) to those facing the user and influencing behaviour: search engines (e.g. Google search), news aggregation services (e.g. Google News), news feeds (Twitter Trending, Facebook's Trending Topics), prognosis/forecast (e.g. Google Trends), news scoring (e.g. Reddit, Digg), content production (e.g. Quakebot, Quill). Bias, discrimination, and the secret nature of data processing and algorithms (Pasquale 2015; Noble 2018) were originally discussed in the context of search engines and recommendation systems for shopping and for entertainment online, but the debacle expanded to large-scale electoral propaganda and public opinion influencing in 2016 and 2017, when data-sharing practices among companies started to be scrutinized.

Following the Facebook–Cambridge Analytica scandal, algorithm-driven decision-making is currently regarded as a threat to democratic processes, highlighting a number of concerns: the covert manner in which personal data is collected, processed, and rendered profitable by companies without the consent of the data subjects; the opacity of the data sharing practices in the private sector; the increasingly more sophisticated tools applied by self-learning algorithms in decision-making. Different from supervised machine learning, which predicts an output based on the data input, more responsibility is assigned to a computer program in unsupervised and in reinforced learning. The former is often deployed to structure large datasets based on pre-defined features, whereas the latter allows the computer to learn how to behave in a new environment, based on constant feedback (Article 19 and Privacy International 2018).

In his responses to the US Congress inquiry held in April 2018 on social media manipulation during the US 2016 presidential election, Facebook's CEO Mark Zuckerberg made frequent references to a solution his company invests in to tackle misinformation on its platforms: perfecting AI to automatically recognize and remove unwanted content. Using algorithms to police the Web, be it based on user feedback via flagging (Caplan and Boyd 2016) or in an automated manner, is in no way new to the operations of Internet companies. This practice is applied across the board to abide by national legislation or to address copyright infringement, among others. Yet deploying it uniformly for addressing social problems does not epitomize a solution-driven, people-centred approach, but reinforces the technological determinism credo dominating the Silicon Valley. This may do more harm in the long-term.

Distrust in the power of companies to protect their users' information first appeared as a generalized concern around the 2013 Snowden revelations and continued with a staggering number of data breaches over the following years, resulting in the disclosure or misuse of billions of online personal records. In 2017 alone, there were 5,207 breaches reported, exposing approximately 7.89 billion records, an increase of about 24 per cent compared to the previous year (Risk Placement Services 2018). Alongside hacks and accidental publications of data, personal information has also been progressively compromised in cyberattacks. In May 2017, the WannaCry ransomware attack affected more than 200,000 computers in 150 countries, followed by other attacks equally disruptive. The vulnerability exploited in this attack on Windows systems paralysed the National Health System in the United Kingdom, where an important number of hospitals were using an older, unpatched version of the operating system produced by Microsoft.

The call to restore trust in the Internet, first placed on the global agenda in 2013 by technical bodies and later by international organizations, was heard over and over again. Since 2015, it was in connection with cybersecurity norms. What was different this time was the authoritative proposal coming from companies to look for solutions together with governments. In addition to voluntary initiatives, corporations like Microsoft or Google provided unilaterally drafted norms for a Digital Geneva Convention and for digital security and due process, respectively. The role of Microsoft as a norm entrepreneur was highly prominent in the last two years, due in particular to its attempts to socialize the proposal in the UN framework and among industry players.

Proposing six security principles back in 2014, Microsoft moved in 2017 to a more comprehensive approach to limiting the stockpiling of cyber weapons, building on the humanitarian conventions (to protect civilians in

times of war) signed in Geneva at the turn of the century. At a time when the perceived exceptionalism of the Internet sector is increasingly challenged, this proposal focuses on treating the industry as neutral in cyberattacks, thus permitting user-centred interventions. In his keynote at the UN in Geneva on 14 November 2017, Brad Smith, the President and Chief Legal Officer of Microsoft concluded his speech with the message: 'Cybersecurity needs to be a cause for our times; all communities must contribute and learn from each other to find solutions' (Radu 2017). The next step in Microsoft's efforts was the Cybersecurity Tech Accord introduced in April 2018, a voluntary industry initiative committing to protecting users from malicious attacks by states and criminals. As of June 2018, the Accord had forty-five signatories, including Microsoft, Facebook, LinkedIn, Nokia, Telefonica, Cisco, and Dell. States have so far been reluctant to endorse the Digital Geneva Convention proposal.

In the area of AI, a similarly powerful call has been made by industry players to governments around the world. In 2017, 116 technology leaders and founders of robotics and AI companies from twenty-six countries, including Google DeepMind's Mustafa Suleyman and Elon Musk, the American inventor and engineer behind Space X and Tesla, sent a petition to the UN to call for new regulation on the development of AI weapons and an explicit ban of lethal autonomous weapon systems (LAWS), or killer robots. Discussions on this are ongoing in the framework of the UN Group of Governmental Experts on LAWS, to which 125 countries (all high contracting parties to the Convention on Certain Conventional Weapons) are participating.

This new exercise of power, coalescing around the introduction of norms that can be agreed cross-sector, is indicative of the current search for basic consensus and norms around the conduct of war in the cyberspace. As of 2018, a form of legalization compatible with current business models continues to be sought by big Internet companies, but also by states, in a space dominated by limited means to attribute attacks, informal governance, and ad hoc arrangements. The next section turns to the position of governments in these discussions, presenting different and sometimes conflicting conceptions of power in IG, be it in material or social power terms.

Stronger National Approaches

The growth of the Internet has long been steered by the Pentagon and that represented one of the core power contests in IG. Post-2015, a differentiation of approaches is visible, in particular due to the increased prominence of regional groups and developing nations, in the context of the Trump-led

withdrawal of the United States from Internet policy. Around the IANA stewardship transition, Powers and Jablonski assessed that 'the United States no longer has the diplomatic, military or economic capital to compel international compliance with its unilateral control over the world's most critical medium' (2015, 130). Cybersecurity is one of the fields where responsibilities have been re-assessed under President Trump. The position of US cybersecurity coordinator, introduced under President Obama in 2009, was abolished by the National Security Council in May 2018, when the portfolio was delegated to a deputy (Kornbluh 2018).

Importantly, as national governments have defined more clearly their interests, the interaction with the private sector has changed. Many states have increased their cyber capabilities for both offensive and defensive operations (Radunovic 2017a) and modelled their relationship with the private sector as a delegated authority one. Not only are companies policing the Web on behalf of states, but they also execute complete Internet shutdowns at the request of governments, a phenomenon ever more common after the Arab Spring. The NGO AccessNow (2018) documented 108 instances of blackouts in 2017, the majority of which took place in Asia and Africa. The reasons offered by governments for these intentional disruptions of service or connectivity range from ensuring public safety and limiting mobilization during election times to preventing cheating in school exams. In the first half of 2017, Google, Facebook, and Twitter received a total of 114,169 requests to remove content from seventy-eight countries and 179,180 requests for information about Internet users from 110 countries (Horejsova et al. 2018, 9).

Acting as a regional bloc, the EU introduced the General Data Protection Regulation (GDPR) governing the privacy, the protection, and the transfer of data of European citizens. The regulation entered into force on 25 May 2018 and harmonized the data regimes across all member states, setting a standard to be pursued inside and outside the European border by both public and private institutions. In effect, a number of countries such as Argentina, Brazil, South Korea, or Tunisia have adopted or are discussing the adoption of legislation similar to the GDPR, leading to an expansion of the model to the Global South.

Among the GDPR innovative aspects are: the focus on the explicit consent of the user, the right to rectification and erasure of information, as well as the right to explanation. The latter mandates that 'meaningful information about the logic' of automated systems is provided when a request is made by the data subject, together with an explanation of the significance and envisaged consequences of the processing thus implemented (Articles 21 and 22). Conceived as a framework for data minimization, the GDPR imposes an obligation to report breaches and introduces a two-tiered sanctions regime: for

non-compliance with important data protection provisions, businesses risk fines imposed by data watchdogs of up to €20 million or 4 per cent of global annual turnover for the preceding financial year, whichever is the greater. For other breaches, fines of up to €10 million or 2 per cent of global annual turnover of companies are envisioned.

In Europe, a strong regional approach was preferred by the Commission for privacy and data protection, whereas for other issue areas, such as the sharing economy, the Court of Justice of the European Union (CJEU) encouraged the development of national approaches. The CJEU judgment from December 2017 settled the long-standing issue of defining the legal status of Uber in an inquiry brought forward by the Barcelona taxi association over misleading practices and acts of unfair competition. Declaring Uber 'a service in the field of transport', rather than an information society one, the court decided that member states can regulate this business model as they see fit under their local laws. While the GDPR allows derogations by member states to fifty different provisions, enabling them to fit their local needs by adjusting certain parameters, the crux of it remains a Brussels-controlled regulation with extraterritorial effect.

On the surge lately, the trend of extraterritoriality derived from domestic regulation has touched the areas of cybersecurity, privacy, and data protection, as well as freedom of expression. More than thirty-five laws were passed since 2015 in thirty-four countries across Europe, Africa, the Americas, the Middle East, and Asia-Pacific (ISOC 2018) in these IG domains, a majority of which focuses on cybersecurity. This points to a move towards an increased securitization of the field worldwide. The international relations (IR) concept of securitization, developed by the Copenhagen School and understood to mean the process through which an issue is presented as posing an existential threat to a designated referent object (Buzan et al. 1998), explains how discursive politics around an issue might justify extraordinary measures to a legitimating audience (Balzacq 2011). Repeated attempts to galvanize support around cyber norms have led to the securitization of IG as a whole in the last couple of years, both rhetorically and in terms of physical changes to the network.

Technical modifications of the infrastructure performed in order to strengthen security and control at the national level have a considerable impact on the global Internet, engendering the long-feared prospect of fragmentation by creating several Internets. China, for example, uses the Source Address Validation Architecture for inspecting the source of the data packets forwarded on the Internet based on an authenticated Internet protocol address that must be authorized, unique, and traceable. This process, using network management, control, and malware avoidance techniques, stops any

communication from unauthorized addresses. Since 2009, Chinese authorities have implemented a real-name registration policy for the country-code top level domain *.cn*, requiring citizens who register domains under *.cn* to provide prior passport identification. Iran and Russia have also announced similar plans to build their own infrastructure and impose strict restrictions on Internet exchanges.

Internationally, rules for the conduct of cyberwar remain a heated topic in state-led forums. Bilateral treaties opposing cyber-espionage and cyberattacks have been on the rise, with wide variations at the level of engagement: strategic partnerships (Canada–Israel), continuous dialogue (EU–Japan), or memorandums of understanding, such as the one between the United Kingdom and Singapore (Radunovic 2017b). Inter-governmental cooperation has been advanced in the framework of regional cooperation and cybersecurity capacity building now has a permanent place on the policy agenda of the Commonwealth, the African Union Commission, the European Union, or the Organization of American States. In the absence of a global consensus on norms of behaviour in the cyberspace, the staggering number of cyberattacks and state defence probing exercises have led different coalitions of states to design their own set of rules. Participation in internationalizing coalitions on security matters is not new, but the focus on cyber aspects has increased tremendously over the last three years. At the international level, both China and Russia have promoted the cyber-sovereignty principle, understood as the right to choose an own path of digital development and to participate on an equal footing in international Internet-related decision-making.

On the one hand, Russia has proposed an international code of conduct for information security, submitted to the UN General Assembly in 2011 and revised in 2015 in the framework of the Shanghai Cooperation Organization (SCO). Russia is expected to propose this code again in the UN in September 2018, following the failure of the dedicated UN Group of Governmental Experts to agree on language endorsing state responsibility and the right to self-defence. On the other hand, NATO recognized the cyberspace as an operational field in 2016; the expert revision of the voluntary Tallinn Manual laying down the applicable international legal norms in cyberspace was completed in 2017.

At the domestic level, Internet-related regulation used to be addressed as part of different ministerial mandates such as telecommunications, economy, foreign policy, or defence. For the longest time, these ministries worked in silos, without a unified approach to Internet policies and with little or no cooperation for deciding or implementing actions together.[1] Participation in

[1] A frequently cited exception was Brazil, where the coordination of most Internet-related activities was primarily achieved via a multi-stakeholder body, the Internet Steering Committee (Comitê

ITU and other international meetings lacked a unitary national vision, which resulted in adopting incoherent positions across subfields of digital policy during international negotiations. This is beginning to change as the Internet is placed higher up on the political agenda.

A number of states have also appointed cyber diplomats (the United States, the United Kingdom, Germany, and Finland were among the first) and have created specific agencies for IG-related actions (the United States, China) aiming to mitigate the lack of consistency in sectoral approaches. A preoccupation for digitization and new technologies has led to concrete frameworks and action plans. In 2017, the United Arab Emirates appointed the first minister for AI, the G20 held two summits for ministers in charge of the digital economy, and Denmark appointed its first ever digital diplomat in the Silicon Valley. IG has been a part of foreign policy for a much longer period of time, but the current developments indicate that—beyond an international (re) distribution of power—tech diplomacy nowadays is supported by domestic political structures.

Just like for companies, the next power struggle among states is leadership in AI. Russian President Vladimir Putin was quoted as saying, in September 2017: 'whoever becomes the leader in this sphere will become the ruler of the world' (RT 2017). By mid-2018, twenty-two countries have either started or completed a process to define their national AI strategies or frameworks with dedicated budgets, including Canada, China, France, India, Japan, Mexico, Singapore, South Korea, the UAE, the United Kingdom, and the United States.

In their report on the rise of the so-called 'techplomacy' in the Bay area, Horejsova et al. 2018 note an increased specialization in the field of diplomacy attuned to particular subfields, such as AI or cybersecurity. The current diplomatic presence in the Silicon Valley takes various forms, from a dedicated tech diplomat (e.g. Denmark), to consular representation and an innovation centre (e.g. Austria, Switzerland, the Netherlands), a state investment promotion agency (e.g. Czech Republic), an honorary consul (e.g. Hungary, Finland) or a separate branch of government (Japan). However, for the time being, most developing countries mediate their relations with the US-based tech industry from their embassy in Washington DC.

China and India, the two largest Internet markets by number of users, pursued different strategies in their profiling as leaders in the IG field. Both countries have seen government-backed progress in Internet technology, yet

Gestor da Internet no Brasil, or CGI.br). Due to the political turmoil in the country, CGI.br has recently come under attack and its approach is likely to suffer changes.

their approaches reflect different core values and future directions. The approaches taken by these two countries deserve a separate discussion below.

China and India

Poised to become the second largest contributor to the UN general budget for the 2019–2021 period, China exerts considerable influence in the key UN sub-agencies covering Internet-related aspects. India, caught in between a multi-stakeholder rhetoric and a state-based approach to IG, has yet to define a consistent approach in its international engagement, be it as part of G20, of the SCO or of the BRICS—Brazil, Russia, India, China, and South Africa.

Beijing has taken the route of trade and investment policies to influence global IG and gained considerable support from other countries via its Belt and Road Initiative. Moreover, in the e-commerce preparations ahead of the WTO Ministerial in 2017, China has co-sponsored (together with Pakistan) a proposal focused on the promotion and facilitation of cross-border trade in goods, payments, and logistics services, maintaining an emphasis on the development dimension. This vision of e-commerce is favourable to its platforms, currently among the largest in the world. The tech trinity known as BAT (Baidu, Tencent, and Alibaba) have recently started investing in or acquiring companies in other industries, including retail, sharing economy, or fintech (Liu 2018). China is also coming second after the United States in international patent applications, the two technology companies topping the global ranking being Huawei and ZTE Corporation (WIPO 2018).

India, on the other hand, has taken an inward look and focused on domestic technological upgrades. It opted for open-source technology in moving its governmental services online, to avoid dependence on private providers and adapt the specifications to the local context. The 'India stack' collection of digital platforms built by the government, together with the digital infrastructure on which it resides, are placed under public oversight. To provide an identification system for Indian residents and facilitate access to governmental services and social benefits, India introduced *Aadhaar*, the world's largest biometric ID system which has over 1.2 billion enrollees now (Nilekani 2018). The introduction of this system in 2009 was mired in fears of privacy breaches, convergence of the data collected across databases, increased surveillance, profiling and targeting, as well as vulnerability to fraud, all of which turned out to be real. More recent debacles drew attention to the use of Aadhaar by private companies (such as telephone companies and banks) and the case was presented in front of the Supreme Court.

A digital national identity card project is also underway in China, where Alibaba and WeChat compete for providing it. After passing strict regulation

in areas such as social media or gaming, China is experimenting with a social credit programme, that rewards good behaviour online and sanctions unwanted behaviour, defined by the government and implemented with the help of companies. The score resulting from public and private records about a citizen's behaviour could be further used to determine opportunities for travelling or employment. Voluntary for the time being, the system will be mandatory as of 2020.

China's July 2017 comprehensive strategy entitled *A Next Generation Artificial Intelligence Development Plan* stresses the aspiration to become the 'world's primary AI innovation centre' by 2030, touching research and development, industrialization, talent development, education and skills acquisition, standard setting and regulations, ethical norms, and security. Deployments of AI are also tested in the military field, in particular for cybersecurity, surveillance, and autonomous drone swarms. For its near-future plan, India embraced the 'AI for all' approach stressing social inclusion alongside economic development. While rhetorically adopting a national approach closer to a public good vision of the Internet, India has yet to show how it can be deployed in a citizen-centred way. Preserving a socio-economic baseline at a time when its top firms providing technical services to brands all over the world—Infosys, Tata Consultancy Services, and Wipro—increasingly resort to automation might bring the country closer to some of the debates in Germany, where a 'third way' between market economy and social welfare is sought in designing the national AI strategy (Hoene 2018).

Preparing to become a 'cyber-superpower' as stressed by President Xi Jinping, China is harnessing the potential of quantum computing in addition to AI. Since the launch of the first ever satellite using quantum cryptography communication in 2016 and the opening of the Beijing-Shanghai Backbone Network (BSBN), the world's first long-distance quantum-secured communication route in 2017, China envisions working closely with its native companies to develop driverless cars, automated medical diagnosis, and smart city management systems.

Conventional approaches to power underline the material or the dominance dimension, but the manifold manifestations of power we have noted here show them alongside implicit or 'soft' forms, such as the ability to shape the agenda and the subsequent global discussions, as well as the ability to form identities and perpetuate communities over time. As far as the classical definition of power goes, the capacity to do something or determine others to do it might not tell the full story in IG. The technological breakthroughs to come and the new authority dynamics they will incorporate can help us develop novel understandings of IG power.

As it continues to transform, the Internet builds on its now-established governance patterns, confirming or dismissing various relations of power. This discussion shows how technology and dominant market positions intertwine to wield new forms of power, with intended and unintended effects. It provides evidence for how a collective representation of a technical project (Flichy 2007) is pre-defined politically and later encapsulated into a vision integrated across all relevant sectors of society. Beyond states and companies, a significant repository of power in the field is the IG community, an agency-loaded space where interests come together to be represented, mediated, heard, and legitimized.

The IG Community

What used to be a community in the hundreds now spans a few thousand people who regularly speak at multiple global events every year, attend most of the preparatory meetings, and participate actively in online discussions. The Internet community has expanded and diversified significantly after the WSIS process. The number of on-site Internet Governance Forum (IGF) participants has increased from around 600 in 2006 to more than 2,000 by 2017. The Internet Corporation for Assigned Names and Numbers (ICANN) and IETF meetings regularly gather about 2,000 people, a number of attendees similar to the annual WSIS Forum. The NetMundial event hosted by Brazil in 2014 brought together more than 1,200 representatives of different sectors, whereas the Wuzhen Internet Summit convened by the Chinese Internet Information Office had approximately 1,000 participants in 2014 and twice as many in 2015. Business-led events like the annual Mobile World Congress organized by the Global System for Mobile Communication Association (GSMA) in Barcelona every end of February, attract close to 100,000 attendees. The key players from the industry also participate as sponsors and send delegates to most Internet gatherings.

Apart from global events, active IG members are generally also involved in activities led by regional organizations like the Council of Europe, the Association of Southeast Asian Nations (ASEAN), the EU, or the African Union, and run or participate in the twelve regional and seventy-six national IGFs. While the target group for each of these meetings might differ, there is extensive overlap of participants, indicating that a core community has formed. The ability of participants with different skills and backgrounds to contribute to discussions on highly specialized IG topics was enhanced over time through better and easier access to resources, demands for more

transparency in the process and, in some cases, financial support to attend face-to-face meetings.

In the early days of the Internet, following the wording of the RFCs, 'community' was the preferred referent for the grouping of volunteers, enthusiasts, and experts closely associated with a particular process. Generally, they were joining the discussion in an individual capacity. Currently, the term is used to refer to those professionally engaged in the development of the Internet, on the policy or technical side, in a wider sense or for delineating constituencies, as in the case of ICANN or Number Resource Organization (NRO). In conferences and meetings, it has become customary to use the stakeholder grouping to distinguish between participants belonging to various communities (governments, businesses, civil society and technical community, academia), often by assigning them different colour name tags. The representatives of these groups were self-selected in the beginning, yet procedures for nominations and approval have been subsequently institutionalized, spanning different degrees of formality.

Physical participation in IG meetings that rotate across the globe is highly valued, requiring significant commitment of time, energy, and resources. Despite the distributed, virtual modalities of work adopted in between meetings, the knowledge-sharing process and its socially situated nature is reinforced in face-to-face encounters. This results in a pattern of attendance favouring the 'information rich', which not only perpetuates, but also increases the inequality of power and influence. Moreover, this phenomenon tends to favour the over-representation of corporate actors, who are more incentivized to participate in physical meetings as part of their lobbying and marketing efforts. Despite repeated calls for inclusiveness, the under-representation of developing countries in the IG community remained a constant throughout the WSIS decade and it has only come to be addressed when formal mechanisms of selection were introduced to ensure a balanced representation of all regions. The unequal access was partly due to a reliance on volunteer work, the mark of native Internet institutions, as opposed to the principle of uniform representation of all member states in intergovernmental settings.

With the steady increase in the number of global meetings, patterns of participation are more difficult to distil, and it is oftentimes complicated to assign one pre-defined sector-based identity to some of the early participants in IG processes. After the creation of ICANN, when the meaning of 'community' was formalized, categorizations by sector and orientation were popular: for example, business community, non-commercial stakeholder community. In its communication related to the IANA stewardship transition in March 2014, the National Telecommunication and Information Administration (NTIA) referred to the 'global multistakeholder community',

leaving it up to those involved in the process to specify what that might mean. Consequently, an intricate process to define the various interests, affected communities, and representatives was set in motion, which ultimately led to a proposal to form an 'empowered community' as a check-and-balance mechanism, discussed below.

Communities in the IANA Stewardship Transition

A new governance process was set in motion a month before NetMundial, on 14 March 2014, when the Department of Commerce's NTIA announced its intent to transition the IANA oversight function to the 'global multistakeholder community'. The US government contract with ICANN over the coordination of the Internet's technical resources specified the former's stewardship role over the domain name system (DNS)—a role entrusted to the NTIA. According to this agreement, for any change in the DNS root zone, such as the introduction of a new top level domain, ICANN would need a validation from the NTIA before execution. The NTIA, in turn, would check that ICANN's decision respected its policies and would ask Verisign (the private company maintaining the root zone) to implement. Importantly, the fact that there had not been any instances of non-approval by NTIA throughout the duration of the contract showed the political dimension of the discussion, building on the legacy of early-day discontent with ICANN.

What became known as the IANA stewardship transition process was initially intended to be finalized by 30 September 2015, but was extended until September 2016. Similarly to the 1998 process resulting in the creation of ICANN, the NTIA established a set of *sine qua non* conditions for the transition: first, to obtain a broad community support; second, to adhere to the following four principles: support and enhance the multi-stakeholder model; maintain the security, stability, and resiliency of the Internet DNS; meet the needs and expectations of the global customers and partners of the IANA services; and maintain the openness of the Internet. ICANN acted on this announcement by issuing a scoping document on 8 April 2014 and fostering a month-long consultation on the next steps.

Refocusing attention away from the surveillance debates and back to the legitimacy and accountability of ICANN, the IANA stewardship transition process involved a large number of active ICANN participants serving in a voluntary capacity, as well as a number of observers from different walks of life. Of the volunteers, thirty members joined the IANA Stewardship Transition Cooperation Group (ICG) and acted as liaisons for thirteen different stakeholder communities within the corporation. To agree on a final proposal for

the review of the NTIA, the coordination body thus formed had the mission of compiling the proposals developed independently by the communities directly affected by the transition: the Protocol Parameters community, the Numbers Resources community, and the Domain Names community. Table 6 provides an overview of the proposals put forward.

Of these proposals, the most controversial was the naming-related one, which linked the transition to a planned ICANN accountability reform.

Table 6 Comparison of the proposals of ICANN communities for the IANA stewardship transition

	Protocol parameters community	Numbering resources community	Domain names community
Functions	IP parameters	Management and distribution of numbering resources	Naming-related
Proposal submitted	*6 January 2015*	*15 January 2015*	*25 June 2015*
Proposal issued by	IANAPLAN Working Group (IETF and IAB)	Consolidated RIR IANA Stewardship Proposal Team (NRO, ASO, and RIRs)	Cross Community Working Group (GNSO and ccNSO)
Substance of the final proposal	IANA protocol parameters registry updates to continue to function as before. To continue to rely on the system of agreements, policies, oversight mechanisms created by the IETF, ICANN, and IAB for the provision of the protocols parameters-related IANA functions.	ICANN to continue to serve as the IANA functions operator for number resources and perform those services under a contract with the five RIRs. A contractual Service Level Agreement (SLA) to be established between the Regional Internet Registries and the IANA Numbering Services Operator. A Review Committee (RC) to be formed (community representatives from each region) to advise the RIRs on the performance of the IANA functions operator.	Form a new, separate legal entity, Post-Transition IANA (PTI), as an affiliate of ICANN to enter into contract with ICANN for the operation of the IANA functions. Create a Customer Standing Committee (CSC) responsible for monitoring the operator's performance as per contractual requirements and service level expectations. Establish a multi-stakeholder IANA Function Review process (IFR) to conduct reviews of the performance of the naming functions. ICANN's legal jurisdiction remains unchanged.

Work on the latter started in May 2014 and led to the formation of the Cross-Community Working Group on Enhancing ICANN Accountability (CCWG-Accountability) in October that year. The group divided the work into two parallel streams, the first comprising the prerequisites for the IANA transition (to be completed before the end of the NTIA contract), and the second extending reforms beyond the transition. To establish a clear division between the technical and policymaking functions, the proposal submitted by the ICG to the NTIA recommended that a separate legal entity take over the role of IANA functions operator, back then referred to as Post-Transition IANA. When the entity was legally incorporated in California in August 2016, the name changed to Public Technical Identifiers. Two more committees were created ahead of the transition, namely the Customer Standing Committee and the Root Zone Evolution Review Committee, together performing the oversight function previously entrusted to the NTIA.

Different drafts for the accountability architecture proposed by the CCWG-Accountability were developed by the group and were open to public comment at different stages. The last one of them, further refined, proposed that a new entity, 'the empowered community', be created as a California unincorporated association, comprising all existing supporting organizations within ICANN, plus the Governmental Advisory Committee and the At-Large Advisory Committee—representing end-users. The envisioned empowered community, to be consulted before key pronouncements, would have a veto power over a number of decisions by the ICANN Board in case of dissatisfaction. Among these were: the budgets or strategic/operating plans, changes to ICANN standard by-laws and fundamental by-laws, status of individual Board members or the entire Board, and Board decision-making related to reviews of the IANA functions.

Despite a few legal challenges that made the transition uncertain until the day before,[2] the process leading up to the removal of the NTIA oversight over ICANN concluded on 1 October 2016, when the IANA contract between the two entities expired and the new IANA functions set-up was introduced. The added-value of the transition process was the initiation of a much broader dialogue on the accountability of ICANN. While the minimum accountability prerequisites materialized for the transition to happen,

[2] Among the most important of these was the lawsuit filed on 28 September by state attorneys general in Arizona, Texas, Oklahoma, and Nevada asking a federal district court to issue a temporary restraining order preventing the contract to expire on 30 September 2016. The arguments put forward revolved around considerations for potential freedom of speech risks and disposal of US property without congressional approval.

discussions continue around larger reforms and ways to strengthen ICANN's accountability towards the broader community.

In the IANA stewardship process, the role of the community was rethought and brought forward along new dimensions, unique in this space. It remains to be seen what power differentials emerge in the implementation of this ambitious project. This way of involving the transnational policy network formed around the technical management of the Internet builds on the grand collaboration that has been historically developed by technical bodies with volunteer support. Although ICANN remains under Californian jurisdiction, its legitimacy is no longer challenged in the IG architecture.

Various Meanings of Community

The World Wide Web (WWW) expanded and changed tremendously through the collective work of public interest groups, originally formed to tackle the technical issues emerging from networking. Later on, content and software developers employed by companies joined the initial groups to bring their contribution to the development of standards. Unpacking the community referent for the key Internet institutions shows that business orientation has remained strong in technical meetings dedicated to the Internet standards. In the work of the IETF, anyone could participate in the development or proposition of a standard, according to the published rules and procedures, by signing up as a volunteer to one of the working groups. However, technical expertise constituted an essential prerequisite for effective participation, and that indirectly led to an overrepresentation of participants regularly involved in its processes.

In recent years, a new significance has been attributed to the 'community' referent: dominant businesses such as Facebook have started employing it to designate the group of people drawing the rules of behaviour on its platforms. These standards are established by a 'faceless' group made up of content policy team members at Facebook in eleven offices around the world (Facebook 2018). The guidelines are revised regularly and implemented in the content moderation activities, including flagging content, filtering, or taking it down, tasks performed by combining AI tools, manual reviews, and reports from users. The Community Operations team implementing these standards works with more than 7,500 content reviewers in forty languages. But in spring 2018, the Community guidelines were deemed insufficient by many international organizations and governments, which started scrutinizing the role of Facebook in furthering abusive behaviour and hate speech, and inciting violence in a number of developing countries (Taub and Fisher 2018). In

Myanmar, Indonesia, India, and Mexico, the amplifying effect of hate speech on Facebook led to the murdering of tens of people.

Local values representation is the second point of contention towards the Facebook community. The unilateral definition of what is and what is not acceptable online by a company headquartered in the United States is harder to sustain as more than 2 billion people use the platform. Facebook's largest user base at the moment is in India, but little of the social and cultural norms there appear to transpire in the global policy of the company, despite the reinforced presence of Facebook's public policy team at all major IG events. In designing community standards, how much should reflect the community itself and be tailored to the local context? Will a global approach, designed by Facebook employees, together with invited experts and selected advocacy groups, be sufficient to avoid tragedies like the loss of human lives?

The initial Internet community was formed around a number of principles defined in a participatory manner by the contributors to the network. Their approach had little to do with form-filling and bureaucracy and more to do with achieving rough consensus by ignoring extreme views. However, the gradual institutionalization of the field resulted in having some of the early members in favour of (more) procedural approaches to designating representatives or appointing the leadership. The legitimacy and accountability discourses, more frequently heard in state-dominated forums, became central to the core Internet community, often with regards to the selection of delegates for higher fora.

At the outset, core communities were rather easy to identify through their membership arrangements and specified objectives, whereas nowadays the categorization is no longer as strict. The most active participants in ICANN and the Working Group on Internet Governance (WGIG) were also frequent speakers at the IGF and have been members of the Multistakeholder Advisory Group (MAG). Mueller (2006) provided a detailed summary of the ICANN-related appointees in the MAG for the organization of the first IGF:

> Two (Alejandro Pisanty and Veni Markovski) are sitting ICANN Board members; one (Theresa Swineheart) is an ICANN staff member; two more (Nii Quaynor and Masanobu Katoh) are former ICANN Board members; two (Chris Disspain and Emily Taylor) represent ccTLD operators; two (Raul Echeberria and Adiel Akplogan) represent Regional Internet Address Registries (RIRs). Even the public interest or 'civil society' representatives are long time players in the ICANN sandbox: Adam Peake of Glocom, Robin Gross of IP Justice, Jeanette Hofmann of WZ Berlin, and Erick Iriarte of Alfa-Redi are all associated with either ICANN's At Large Advisory Committee or its Noncommercial Users Constituency (or both). To that one can add an IETF representative, Patrik Faltstrom, often utilised by ICANN as a consultant, and the Internet Society's public policy advocate. (Mueller 2006)

Twelve years later, the same participants are still highly active in multiple Internet processes. While asserting one identity is important within the community for guiding interpretation schemes, many in the core group wear 'different hats', that is, have multiple affiliations. Most of the time, especially in less formal venues, they start their introduction by mentioning that. Such instances have become widely common and widely accepted in the IG space. Independent of their affiliation, they remain highly vocal on IG issues and procedures no matter what 'hat' they put on. Over time, they have not only taken on board legal, social, and technical issues, but have also been involved in or contributed to defining the ethics of the community. The boundaries between individual and institutional identities are rather difficult to draw for some of the charismatic leaders in the broader IG community. Occasionally, the positions they take may be contradictory: critics of intergovernmentalism often actively participate in the work of the Organisation for Economic Co-operation and Development (OECD) or serve as experts for the ITU.

Among the technical bodies that refer to their communities, two stand out: the World Wide Web Consortium (W3C) and the IETF. The W3C has introduced the possibility of creating Community and Business Groups open to anyone willing to join, free of charge. To lower barriers to individual participation, this initiative addresses Web stakeholders that would connect to the well-established international W3C community for creating open Web technologies. Such Community and Business Groups can be started with a short scope statement and a minimum number of supporters; the general criteria to abide by are the following: open to all without a fee, publicly visible, without time limit, intellectual property rights balanced, and tuned for transition to standards.

The IETF, on the other hand, has built its identity around the values of volunteerism and collaboration, but also informality. Its three meetings held yearly are week-long 'gatherings of the tribes'. The Tao of the IETF, updated several times, even included in its 1993 version a dress code paragraph:

> Many newcomers are often embarrassed when they show up Monday morning in suits, to discover that everybody else is wearing T-shirts, jeans (shorts, if weather permits) and sandals. There are those in the IETF who refuse to wear anything other than suits. Fortunately, they are well known (for other reasons) so they are forgiven this particular idiosyncrasy. (Malkin 1993)

While social interactions are important variables for collaboration, the guide for newcomers does more than simply outline the rules. It builds the expectations of similar practices being preserved in the future by shaping the behaviour of leaders selected among their younger attendees. As they are

encouraged to volunteer to be part of working groups, observing closely the attire of the more senior members has had a long-lasting influence.

When it comes to decision-making, the IETF rule of approving standards only after having the rough consensus at meetings endorsed on working group mailing lists was not emulated in other forums. Decisions regarding the public policy aspects of IG remained mostly confined to face-to-face meetings, with a minimum use of online collaborative platforms bridging the different stakeholder groups (Radu et al. 2015, 5). Although there is an intense use of mailing lists and e-participation tools for the exchange of ideas and (statement) coordination, they remain limited to the internal workings of a specific community (e.g. IG Caucus, BestBits for civil society groups) or a specific process (e.g. one of the IGF Dynamic Coalitions, various ICANN-related initiatives). A number of attempts to enhance cross-community communication on broad IG discussions—such as the 1net or the NetMundial initiative—have been short-lived, failing to engage key actors and substantiate actions in the aftermath of the physical meetings they were created for.

Old-timers and Newcomers

By and large, in the group dynamics, the small number of active participants—primarily established players or 'old-timers'—defines the rules for the larger passive membership. Key individuals thus become cultural and social containers, who produce, perpetuate, restate, or transform discourse. They represent the locus of power and have extensive leverage over the relationships formed with the newcomers, in particular by recruiting some of the younger participants, having a say in structuring their access and defining the transparency procedures introduced by the group. Gaining full recognition in the community comes after following a well-defined trajectory in the group, which generally starts with smaller project involvement and ends with a move towards the centre of the community for those most motivated. Along the way, a gradual, but steady identification with the community practices and acquisition of the jargon and vocabulary becomes the norm.

The expansion of the IG communities is closely linked to the process of designing guidelines and codes of conduct for newcomers, as a way to bridge the constant tension between the insiders of a shared practice and newly arrived members. Modelling becomes the main vehicle for shaping the community: as procedures grow ever more complex, most organizations introduce (and fund) newcomer programmes, in most cases targeting participants from developing countries. Examples of such initiatives include the IETF and ICANN fellowships to their meetings and ISOC ambassadorships

to the IGF, aiming to bridge the gap between the 'information rich' and the 'information poor' and to give a voice to regions and stakeholder groups that are underrepresented, but also to immerse novices in the work of these institutions. ICANN also runs a Community Onboarding programme, while ISOC funds travelling of young people to global events via its NextGen programme. These activities are supplemented by online courses—like the ones ran by DiploFoundation or Internet Society—and opportunities to be involved in regional events. As embedded experiences, these programmes not only inform about praxis, but also immerse the newcomers in full-fledged, continuous discussions, in particular as they encourage repeated participation.[3] In the process, the newcomers become practitioners themselves.

Early on, in the technical groups, maximizing inclusion was key for ensuring that the standards were interoperable and satisfactory for those most likely to make use of them. Similarly, the adherence to multi-stakeholder processes has since been fostered into community-building processes, for example, in the way in which the ICANN and ISOC fellowships are structured—members of different communities being funded to participate and spend a week together in formal and informal settings. The personal relations established this way increase the trust different stakeholders have in the people they have bonded with informally. Unlike meetings with binding outcomes, the IGF and the WSIS Forum running for a few consecutive days provide a more relaxed atmosphere conducive to personal discussions and informal consultations. Alongside workshops and sessions, participants can attend tutorials, presentations, and, most importantly, hallway conversations concerning actual decision-making processes at the national, regional, or global level.

It is important to note here that the intergovernmental arrangements no longer stand in opposition with the *sui generis* grouping of Internet organizations in their standard-setting procedures or in their operation. They often collaborate, exchange ideas, and check the activities of other organizations in order to improve their inclusiveness and participation practices. Sometimes, the same individuals are behind such initiatives as initiators or proposers. The development of the Internet's technical standards and protocols has been conducted in an open manner, with the involvement of an expanding community encouraged to participate at different levels, and bodies like the ITU-Telecommunication Standardization Sector (ITU-T) have followed suit in adopting a similar approach to tutorials for newcomers, while preserving the solid role for governments specific to state-led processes.

[3] First-time participants in an ICANN fellowship are eligible for two more fellowships to future meetings, whereas some of ISOC's IGF ambassadors are eligible for funding twice.

The interdependence of Internet activities and the increasingly diverse backgrounds of those carrying them out gradually made any idea of acting in isolation fade away. The complementary skills and knowledge of various members, as well as their multi-membership across IG groups were considered a gain for the community. The expansion of a distributed knowledge base and the continuous effort to promote a consistent vision is reflected in the shared praxis. Various communities have worked on historicizing their experience and have subsequently put in place a wiki or a webpage recounting their progress and influence since formation (ICANN's NCUC, Best Bits, etc.).

The need for cooperation to make the network function translated, at the community level, into the amalgamation of cultures and mindsets (organizational, sectoral, disciplinary, but also national or regional) in solution-oriented activities. The distinctiveness of specific etiquettes of interaction, ranging from a rough-consensus approach to extensive diplomatic deliberations over wording, started to blur as an unchanged core group met regularly around (negotiation) round-tables in different venues. The resulting system of norms and rules is a hybrid incorporating, in a unique mix, diplomatic procedures, private logics, and public interest discourses.

Internal Dynamics

Within the community, what becomes apparent is a clustering of members according to the meetings they attend—a grouping they would re-assert across different venues—further reflecting the close interaction and social ties developed over time. ICANN-goers meet three times a year on different continents, whereas active IGF-ers generally pass through Geneva for an agenda-setting consultation before heading to the global meeting in the host country. The WSIS Forum and the CSTD meetings are generally scheduled back-to-back in May every year, allowing some of the participants to attend both. Key members of the community generally take advantage of the IGF schedule to reserve Day 0 for strategic discussions, side events, or public forums, and similar actions have more recently been taken around global gatherings that have not traditionally dealt with the Internet, such as the Human Rights Council's periodic meeting in Geneva.

My immersion in community-building activities over the last eight years allowed me to assess, on multiple occasions, two sets of dynamics that became constitutive of the IG space. The first was the tacit knowledge that community members had about the topics discussed and about each other, visible in the limited explanation about the issues at hand and the use of first names in

formal meetings. The second was the consolidation and repetition of values endorsed by the old-timers.

The absence of introductory preambles and a direct jump into the core discussion without extensive details points to the constant communication that goes on via mailing lists. In this approach, there is an implicit understanding of the knowledge that other members of the group have, their potential contribution, and oftentimes their position in the debate. Moreover, the personal relationships, rivalries, and ideological standpoints are clearly delineated and well-known to everyone in the group, making it easy to assess what coalitions might be formed. As Wenger (1998, 130–31) remarks, sustained mutual relationships—harmonious or conflictual—represent a mark of ongoing interactions; in the IG community, it is not uncommon to start a mailing list interaction by referencing, with minimum information, a long-standing dispute.

Throughout consultations and meetings in formal venues such as the UN headquarters in Geneva, the use of first names was often preferred in lieu of spelling out the full name and affiliation for those who have been involved in IG processes for a long time: Markus, Bertrand, Bill, Avri, Ayesha, etc. This informality made the atmosphere more personal, giving established participants ownership over particular processes. For newcomers though, the practice of calling out personal names indicated a nucleus they were outside of; understanding who the people called by first name were became a rite of passage; it was important to meet them, discuss with them, and eventually become known to them by first name in order to get closer to the nucleus. This applied across sectoral divisions, yet it is important to note that in addressing government representatives the generic delegation formula was preferred (e.g. 'the Chinese delegation'). There were, however, exceptions for the representatives of countries that were most active at the IGF and during its preparatory process: the United Kingdom, Switzerland, France, the United States, and Sweden, whose representatives were also easily recognized by their first names (Epstein 2012, 181).

The second habitual characteristic of the community structuration was the solidification of principles put forward by its key members. Among these, inclusiveness and multi-stakeholder participation were subsequently internalized by the rest of the community. The underlying tenets of the fast-growing Internet community were reproduced in various ways: at recurrent events and through newcomer programmes, through local and transnational anchors, but also through the reiteration of principles that its most influential members upheld. The length of career within the community became a highly valued source of authority, compatible with membership across many other sub-communities. It is from this position that established members promoted

the core values. In their interventions and contributions, the most active individuals frequently referred back to previous meetings they attended, using formulations such as 'I was there when this was discussed/I was a member of the working group/I was chairing the meeting'. Such prefaces reflected different knowledge and commitment levels.

The insights of those more regularly involved gained more weight, not coming in contradiction with their multiple membership across groups endorsing different beliefs. Their ownership claim was rooted in the service done to the community on many other occasions and in their proximity to power structures across different venues, as well as the privileged knowledge they had access to. Importantly, in the IG space, the discussions remained open. The boundaries of the group were maintained insofar as formal representation was concerned, but the different communities acting in this space did not define themselves in contrast with other groups.

Partly explaining this was the far-reaching sharing practice among community members, not limited to work only. Physical meetings offered opportunities to socialize and develop interpersonal relations during lunches, receptions, day-long trips planned together. These informal occasions further contributed to the adoption of a similar vocabulary and the development of a communal knowledge repertoire, which included information about community members, viewpoints, and expectations. The spaces for interaction and the social practices for IG were thus mutually constituted. Socialization shaped the extent to which a shared mindset and the idea of a collective future were perpetuated. As Cohen observed:

> the quintessential referent of community is that its members make, or believe they make, a similar sense of things either generally or with respect to specific and significant interests, and further, that they think that that sense may differ from one made elsewhere. (1985, 16)

Defining a common horizon also meant, in the IG case, an aversion to the exclusion of participants based on their affiliation. It was, for example, common to have business and technical community representatives regularly participating in discussions on the Civil Society Caucus mailing list. In an analysis of the IGF transcripts for the period of 2006 to 2012, DiploFoundation (2015) concluded that the verbal contributions during the annual meetings were divided as follows: 34.45 per cent made by government representatives, 17.23 per cent by NGO representatives, 15.47 per cent by business representatives, 14.60 per cent by the technical community, 11.68 per cent by IO representatives, and 6.57 per cent by academics. Semantically, the contributions of all stakeholders but IOs and academia members were similar, revealing analogous patterns of word usage by the technical community, business

community, and NGOs. This was highly indicative of how relationships have been forged at the nucleus of the community and how daily practices embedded shared-learning processes.

Face-to-face learning, the moulding of a common perspective and the exchange of good practices at global forums also played key roles in shaping the Internet communities in-the-making because they acted as a self-fulfilling prophecy, reiterating the core values in which the identities of the community were rooted. The flexible, self-organizing, English-speaking, male-dominated group that participated in the early days—in ARPANET or in the WSIS process—ossified as a cluster of authoritative voices for the maintenance of the structures whose creation they contributed to. More than sharing similar views on the values to be promoted in IG, the nucleus actively used its high profile and influence to advocate for its vision, for example in pleading formally for a renewal of the IGF mandate back in 2014.

To this day, the multi-stakeholder construct remains deeply ingrained in the principles put forward for institutional design, as it was the case for the creation of the IGF, or for opposing initiatives for not being inclusive enough. Recurrent, structured interactions and interrelations define the core community and reiterate the principles that unite them, limiting the radical discourses. In that sense, multi-stakeholder processes are 'enabling and including, but also disciplining' (Raboy et al. 2010, 84). Actors construct themselves based on their acquired affiliation(s), but also as contributors to the community. They often sit on Advisory Boards together, being habituated into specialized practices in similar ways. Peer reviewers, often called in for collective drafting exercises, are appreciated for both subject-matter expertise and immersion in community practices.

Over time, the process of assigning fixed identities taking into account geographic and community representation was institutionalized. From the selection of ICANN board members to the WGIG members and to the Board of the NetMundial Initiative, the institutionalization of procedures became a central discussion in the community. Procedural design consolidated the claim to representativeness and gave the community a sense of the preferences, ideas, and principles selected individuals would stand for, rather than providing a clear understanding of the arguments that would be put forward in the negotiation. For example, the ample consultation processes taking place within civil society groups served a legitimating purpose, alongside the functional approach to selecting speakers and delegates. The nominations were usually put forward on the mailing list and there was a transparent candidature process, followed by the expression of support and endorsement from the other members of the group, most of the times taking the form of '+1' for the preferred candidate.

Socialized in this practice originally developed by the technical community, the younger active members of the core IG community reproduce and perpetuate it. As Djelic and Quack put it:

> Ultimately, socialization can lead to a transparency of structuring and institutional frameworks and thus to 'invisible' reproduction. This is probably one of the most powerful kinds of stabilization mechanisms, suggesting profound entrenchment and generating great legitimacy. (2007, 165)

The discussion above indicates that neither the community, nor the group belongingness remains static. The meaning and the accepted forms of community participation have solidified and institutionalized in the process, but are by no means fixed. While deliberate effort was put into community expansion—through capacity building programmes, summer schools, newcomer guides, and the mutual orientation of members—social interactions and collective drafting of rules of conduct provided the basis for maintaining the core group. The dynamism of the IG nucleus stems, in part, from the continuous reiteration of common principles and aspirations. But it is also reactionary, as fast responses are required for technical developments and regulatory moves. To participate in fluid configurations of governance, the core community enacts structures of signification and legitimation by drawing on praxis, expertise and lengthy involvement in IG processes.

Anchoring Practices

As discussed in the opening chapter, the IG scholarship has spent considerable time focusing on institutions and novel mechanisms at the expense of comprehensive analyses of practices. This book breaks away with that tradition by integrating practices as an additional dimension of empirical investigation, to reveal how actors coalesce around routines and meanings in their daily work. Anchoring practices are solidified habits turned into pillars for community formation. They represent instances of power perpetuation, reinforcing broader governance structures. Each one of the three anchoring practices identified here is specific to a period, but it is perpetuated beyond, enduring over the years: by 2018, more than 8,400 RFCs had been issued, thousands of multi-stakeholder events took place, and hundreds of ad hoc expert groups completed their IG work.

Importantly, these three practices are also instances of co-regulatory routines consonant with broader contemporary governance arrangements. First, the RFCs emerged in the early days of the Internet and became authoritative in the 1980s to help standardize the first protocols and foster communication

within the technical and academic community working on the precursor of the Internet. Moreover, they helped embed particular values about how things should be done, and what should be prioritized in the process. Second, multi-stakeholder routines were championed around the creation of ICANN and became dominant in the privatization decade up until 2003–2005, when they were sanctioned in the Tunis Agenda. Third, ad hoc expert bodies were more often deployed post-WSIS to legitimize a set of punctual solutions that generally did not challenge the status quo. While they all used to depend on a few active individuals, the anchoring practices explored here are now formalized and institutionalized. To a large extent, the move towards entrenching detailed procedures has shifted the focus from the substance and content of debates to the bureaucratic processes around them.

Influential routines generally enact ideological elements. The different mechanisms of governance at work become structural conditions for social practices framing the rules of the game. In that sense, routine interactions are guided by deeper political endeavours—be they reinforcing or breaking away with established rules—in daily enactments of governance. In the IG community, the neoliberal, market-enabling understanding of the space (Flichy 2007) stood at the basis of the multi-stakeholder discourse. In nascent issue domains, where no textbook approach is possible, substantive expertise is closely linked to the interaction with the groups which possess and produce the expert knowledge. This practice makes it difficult to draw the line between the embodiment of an ideological credo and a genuine participatory approach to governance, as it conflates various dimensions by legitimizing the presence and disciplining the actions of particular actors around the negotiation table.

The creation of ad hoc expert groups speaks to the hierarchy of knowledge established in the community. It therefore performs a separation between those who possess the expertise and are entitled to speak on behalf of different groups and the rest of the community members. While the selection would also be driven by formal considerations such as the representation of different geographical areas and sectors, the expectation of having political stances represented is taken for granted. The practice has become widespread within the EU, with a number of high-level expert groups being formed since 2016: High Level Group on Internet Governance (2016), on Radicalisation (2017), on Fake News (2018), and on Artificial Intelligence (2018). In the same vein, the International Labour Organization (ILO) has established a Global Commission on the Future of Work, chaired by Ameenah Gurib-Fakim, President of the Republic of Mauritius, and by Stefan Löfven, Prime Minister of Sweden. The Commission is expected to produce an independent report in 2019 on digitalization, jobs and social justice. Most prominent among this new set of initiatives is that of the UN Secretary General António

Guterres, who appointed in July 2018 a High-Level Commission on Digital Cooperation, chaired by Melissa Gates and Jack Ma, for a nine-month-long mandate.

Encoding the dominant meanings, anchoring practices are key to understanding the evolution of an issue domain, in particular as they embody rules which are not codified as such formally. They rely on common knowledge, which implies that they 'do not require the time or repetition that habits require, but rather the visible, public enactment of new patterns so that "everyone can see" that everyone else has seen that things have changed' (Swidler 2001, 87). The way communities reiterate practices of recognition and celebrate their members is a case in point here. Starting in 1999, ISOC has been awarding, on an annual basis, the Jonathan B. Postel Service Award. The award, presented at an IETF meeting, goes to an individual or organization with an outstanding contribution to the data communications community. In the selection of the awardee, particular attention is paid to 'candidates who have supported and enabled others in addition to their own specific actions' (ISOC 2015b). Similarly, ICANN's Multistakeholder Ethos Award was launched in June 2014 in London to recognize the leaders of the community promoting multi-stakeholderism within the organization by serving it—for at least five years—in different roles and collaborating across supporting organizations and/or advisory committees.

As the call for nominations details, the Multistakeholder Ethos Award 'recognises ICANN participants who have deeply invested in consensus-based solutions, acknowledging the importance of ICANN's multistakeholder model of Internet governance, and contributed in a substantive way to the higher interests of ICANN's organisation and its community' (ICANN 2015). This annual practice reiterates the need to strive for consensus in ICANN-related activities; but it goes further than that. Just like the ISOC award, it also upholds peer recognition as highly valuable, since the nomination and the review of candidate profiles is done by (a panel of) community members.

Anchoring practices in IG, as evidenced throughout the evolution of the field, reflect the merging of two forms of authority: social and epistemic. On the one hand, group belongingness entitles certain individuals to take part in Internet-related processes. On the other hand, expertise grounded in subject-matter knowledge becomes more appreciated over time. Different IG groups are both rule-makers and targets of rules. In a nutshell, anchoring practices are also an important proxy for ideological cohesion and community support. A plethora of consultation mechanisms and channels of input exist, both formally and informally, to bridge the divide between the private and the public realms. This provides evidence for the consolidation of a hybrid environment, in which the boundaries of the community are no longer drawn

solely in accordance with the position taken by key actors. In part, it is due to the reproduction of practices of collaboration that have become the 'invisible thread' behind the way in which the community is organized.

Synopsis

Nowadays, the Internet presents multiple sites of authority at different levels, from national to global. While some of the developments that marked the IG evolution post-2015 were direct continuations of processes started before, such as cross-sectoral convergence facilitated by Internet technology, new concerns surfaced as fresh political and legal endeavours to tackle, such as the pursuit of cybersecurity norms or AI. The first part of this chapter investigated the power dynamics at play post-2015, putting into perspective the key governance transformations.

Dominant private companies, on the one hand, and influential governments, on the other, are currently restructuring the debates along realpolitik and economic dimensions. Their actions impose, legitimize, and strengthen what appears to be a contested re-arrangement of power. Carving out a clear-cut regulatory space in a dense institutional ecosystem has long been a national priority, but the stakes increased amidst technological innovation and diversification. A product of public and private collaboration, the Internet does not cease to be a field in search of ethical and legal guiding frameworks as its political standing continues to rise. The repeated calls to develop rules, in particular on cyber-operations and AI, point to the securitization of a significant part of the field.

Shifting attention to agency, the second part of this chapter brought into sharper focus the role of the IG community in structuring a unique field of governance. From the introduction of specific guidance for newcomer programmes to the perpetuation of decision-making processes and the enactment of anchoring practices, the core values passed on reflect the characteristics of the initial group of technical bodies, formalized and politicized over time. The dynamics within the community, however, present their own patterns and specificities. In this longitudinal perspective, abstract oppositions frequently applied to IG, such as bottom-up versus top-down, public versus private, state versus market, took on a new meaning. More than articulating a functional, solution-oriented approach to problems, the community patterns identified here are tightly linked to ideological positions, as well as social and epistemic authority. The global IG regime is built on both disruptions and continuities and many different legitimation routes open up in its restructuring.